# Phase estimation using Extended Kalman Filter in continuous-variable quantum key distribution

Arul Prakash Samathuvamani
School of Electronics and Electrical Engineering
University of Leeds
Leeds, United Kingdom
el20a2ps@leeds.ac.uk

Mohsen Razavi
School of Electronics and Electrical Engineering
University of Leeds
Leeds, United Kingdom
M.Razavi@leeds.ac.uk

***Abstract*— Continuous-variable quantum key distribution (CV-QKD) with an independent Local Oscillator (LO) at the receiver offers more security. Carrier Recovery with accurate phase estimation is vital in CV-QKD implementations with independent LO. To overcome the challenges in accurate phase estimation, in this work, we have demonstrated a phase estimation technique with Bayesian filtering, namely Extended Kalman Filter. We have demonstrated that the measured phase noise is around 1.0 x $10^{-4}$. We have also numerically showcased the system's viability by calculating the secret key rate at various conditions. This method of phase tracking reduces the implementation complexity of CV-QKD systems.**

***Keywords—CV-QKD, quantum communication, phase noise, extended Kalman filter.***

## I. Introduction

Advancement in high-performance computing is threatening existing cryptographic techniques. Quantum Key Distribution (QKD), by laws of physics, provides a secure way to transfer cryptographic keys against invades with unlimited technological power and capability [1,2]. QKD provides a secure way to transfer cryptographic keys between Alice and Bob through an insecure channel which is assumed to be in complete control of eavesdropper Eve with unlimited computing power. QKD technology can be mainly categorized into two types. One is Discrete Variable Quantum Key Distribution (DV-QKD) which is based upon the property of single photons, and another is Continuous Variable – Quantum Key Distribution (CV-QKD) based on coherent detection.

In DV-QKD, the secret key is decoded using Single Photon Avalanche Detectors (SPAD), which is expensive and requires extensive optical filtering if the quantum channel is shared with the classical optical channel. In CV-QKD, the secret key information is encoded into coherent states in amplitude and phase quadratures of light. CV-QKD protocol with Gaussian-modulated coherent states (GMCS) based on gaussian-modulated coherent states. GMCS CV-QKD is widely researched because of its potential to offer a cost-effective alternative to DV-QKD. In CV-QKD, P-I-N photodiodes are used to perform coherent detection. CV-QKD can be implemented using existing standard optical components, which makes it a cost-effective alternative to DV-QKD.

One of the main challenges in CV-QKD implementation is to establish a reliable phase reference between Alice and Bob. In this work, we present a technique to estimate the phase of the pilot signal using the Bayesian Filtering technique, more specifically by using Extended Kalman Filter (EKF). Extended Kalman Filter is an iterative algorithm that is used to estimate the value of an unknown variable from a series of known measurements. The main advantage of Kalman Filters when compared to other estimation techniques as it can effectively deal with noisy input data and adjust its weights between measurement of the system and its model estimates. The performance of the estimation technique is verified with the help of numerical simulations at various operating frequencies of the pilot signal. It can be seen that the proposed filtering technique provides more accurate phase estimation and results in a reduced range of phase noise when compared with other phase estimation techniques. The performance of CV-QKD systems is evaluated by calculating various secret key rates at various operating conditions. It can be seen that phase estimation by Extended Kalman Filter gives better key rates when compared with other pilot signal-based phase estimation techniques.

## II. CV-QKD with Locally Generated Local Oscillator (LO) Signal

One of the most researched protocols for implementing CV-QKD is Gaussian Modulated Coherent State (GMCS) protocol. In GMCS, Alice modulates phase and amplitude quadratures of a light pulse from a set of Gaussian random numbers. The prepared coherent state is then transmitted through an insecure channel that is assumed to be fully in control of the eavesdropper Eve. Bob chooses to randomly measure either phase or amplitude quadrature with balanced homodyne or heterodyne detection and informs Alice of his measurements through a secure channel. If the mutual information between Alice and Bob is higher than that of Eve, they go-ahead to perform privacy amplification and error correction. The strong LO signal that is used in coherent detection acts as a selective filter that effectively suppresses noise photons which makes it an extremely appealing solution for implementation in conventional fiber-optic networks.

The GMCS protocol where a strong LO signal is transmitted along with the quantum signal is called Transmitted Local Oscillator (TLO) scheme. However, the TLO scheme carries some major drawbacks. Recent studies have demonstrated that Eve might be able to manipulate the LO by launching sophisticated attacks. Also, in order to achieve shot noise limited coherent detection, the power of the LO signal needs to be 7-8 times higher than that of the quantum signal, which complicated multiplexing and demultiplexing schemes of quantum signal and LO at the receivers end. Also, for implementing CV-QKD for very long distances, an extremely powerful LO signal is needed. Recent studies have been focused on implementing CV-QKD with an LO signal

that is locally generated at the receiver's end. This is known as the Local Local Oscillator (LLO) scheme.

LLO scheme in GMCS CV-QKD requires a reliable phase reference between Alice and Bob. The process of recovering the phase and frequency of the signal is known as carrier recovery. Traditional methods of carrier recovery make use of techniques such as feed-forward carrier recovery, and optical phase-locked loops, etc. These methods of phase estimation cannot be applied to CV-QKD systems as the quantum signals operate in a much lower power regime and have very low tolerable phase noise. Therefore pilot-aided techniques have been studied where low power reference pulses are transmitted alternatively with quantum signals.

## III. Pilot Aided Phase Recovery Scheme with Extended Kalman Filtering

### *A. Pilot Aided Phase Recovery*

In LLO scheme, LO signals are acquired from two separate LO, operating independently at transmitter and receiver. A phase reference signal is generated by Alice and transmitted along with the quantum signals in the same optical path and undergoes the same phase change during transmission. Therefore the phase noise occurring in the signal due to channel transmission is zero. The phase noise in the system is expressed as,

$$\emptyset_{noise} = \emptyset_{error} + \emptyset_{drift} \quad (1)$$

The component $\emptyset_{error}$ comes from the phase difference between LO signal at the receiver and the transmitter. The term $\emptyset_{drift}$ is due to the relative phase drift between two free-running lasers. In order to obtain optimal key rate at long distances, the phase difference between the LO signal at the transmitter and receiver should be kept minimal. In pilot aided phase recovery scheme, to establish a reliable phase reference between transmitter and receiver, Alice sends out a quantum signal along with a relatively strong un-modulated reference pulse from which Bob tries to estimate the phase of the LO using Extended Kalman Filter.

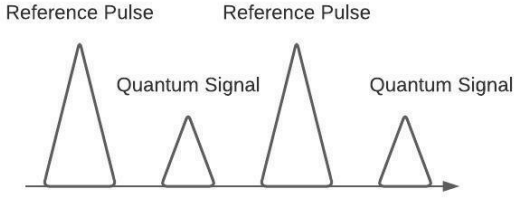


**Figure 1.** *Pilot Aided Phase Recovery with simultaneous reference and quantum signals.*

In order to verify the feasibility of our EKF in CV-QKD applications, the following simulation setup is performed. The simulation is set up as shown in Figure 1. The signal from the MZ modulator is then split into two components by using a beam splitter, one for the reference pulse and another for the signal. In the signal arm, the optical signal is modulated using electro-optic Lithium Niobate Mach Zander (MZ) optical modulator using modulation signals from an Arbitrary Waveform Generator (AWG) and then modulated using Phase Modulator (PM) using the same signals from AWG. The signals are then passed through a Variable Attenuator (VA) to achieve quantum signal strength $V_A$. The reference pulses are delayed using a delay line to align consecutive reference and signal pulses. The reference pulse is then attenuated using a VA. The power of the reference signal is approximately 3.2 times that of the quantum signal.
The signals are then combined and sent through optical fiber channels of varying lengths. At the receiver Bob's end, the signal is passed through a Polarisation Controller (PC) and then passed through a Beam Splitter (BS). Using an LO signal locally generated at Bob's end, Homodyne Detection is performed in the signals. Extended Kalman Filter operation is then performed in the received reference pulses to perform phase estimation operation. The algorithm for Extended Kalman Filtering is explained in the section below.

### *B. Bayesian filtering based on Extended Kalman Filter*

Kalman Filter is a linear estimator for dynamic systems [14]. The state of a dynamic system is given by its state-space model. Kalman Filter works poorly in non-linear systems. Kalman Filter can be extended to estimate in non-linear systems by forming Gaussian estimation of the joint distribution of state x and measurement y. Extended Kalman Filter is based on the Taylor series approximation of the joint distribution [15].

The phase of the pilot signal can be estimated from its noisy measurements of reference pulses by using an Extended Kalman Filter.

The state-space model that describes the phase of the signal is given by,

$$X_k := \emptyset_k = \emptyset_{k-1} + q_{k-1} \quad (1)$$

The state of the symbol at instant '*k*' is given by '$X_K$'. The phase of the system at any instant 'k' is denoted with $\emptyset_k$. The unknown phase noise of the laser system is denoted with $q_{k-1}$ . The phase of the system at any instant is given as the sum of the phase of the system and unknown noise of the system at the previous instant 'k-1'. The phase of the LO signal can fluctuate randomly in a system due to the beating of the LO laser with vacuum fluctuations.The phase noise due to random fluctuations of laser is denoted as process noise in the Kalman Filtering process.

The noisy measurement made by the system is given by the equation,

$$Y_k = A\sin(\Delta\omega T_s + \emptyset_k) + n_k \quad (2)$$

where A is the amplitude of the signal, $\Delta\omega$ is the frequency difference between pilot tone and receiver LO laser, and $T_s$ is the sampling time. The shot noise from the P-I-N detector is given by $n_k$ . $\Delta\omega$ is zero for homodyne detection.

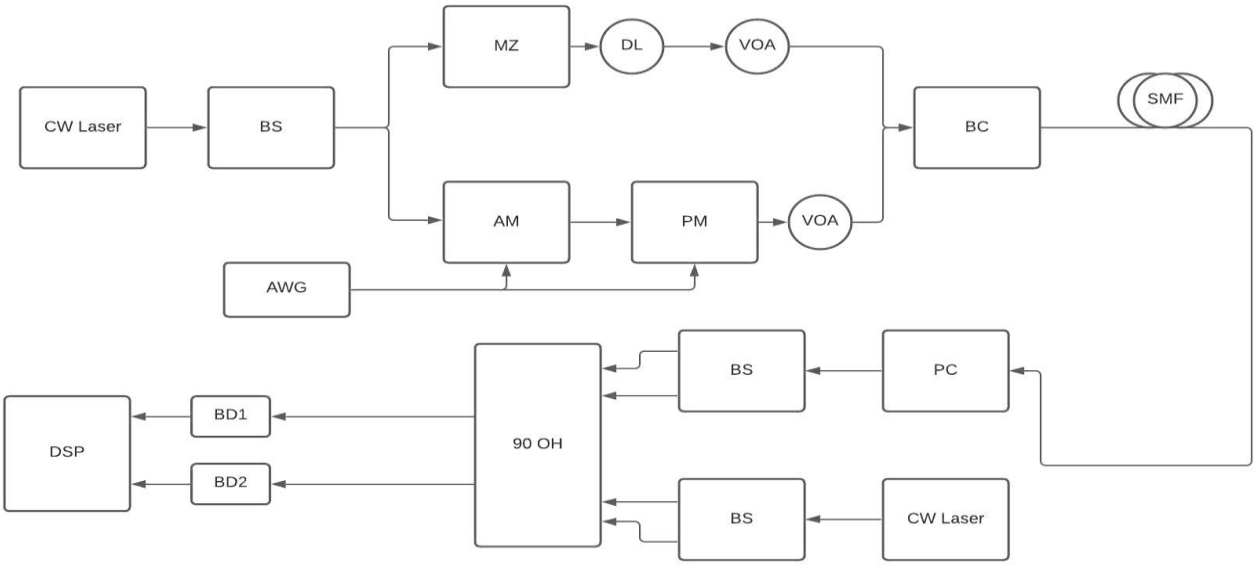


***Figure2.*** *The simulation is set up as shown in the figure above. CW stands for Continuous Wave. BS stands for Beam Splitter. AWG stands for Arbitary Waveform Generator. MZ stands for Mach Zander to modulate reference pulses using a sine wave generator. DL stands for Delay Line. VOA stands for Variable Attenuator. AM stands for Amplitude Modulator using Lithium Niobate electro-optic Mach Zander Modulator. PM stands for Phase Modulator. BC stands for Beam Combiner using X-Coupler. SMF stands for Single Mode Fiber. 90 OH stands for 90$^0$ Optical Hybrid, BD stands for Balanced Detection and EKF is performed in the Digital Signal Processor (DSP). The power of the reference pulses is approximately 3.2 times of that of the quantum signal.*

The EKF filtering model is given by,

$$x_k = f\,(x_{k-1}, k-1) + q_{k-1}$$
$$y_k = h\,(x_k, k) + r_k \qquad (3)$$

where $x_k \in \mathbb{R}^n$ is the state, $y_k \in \mathbb{R}^m$ is the measurement. $q_k \sim N(0, Q_{k-1})$ denotes process noise, and the term $r_k \sim N(0, R_k)$ denotes measurement noise. $q_k$ denotes the covariance of phase noise while $r_k$ gives the covariance of the noise in the measurements. The dynamic model function $f\,(x_{k-1}, k-1)$ of the EKF filtering model is given by equation (1), whereas the measurement function $h\,(x_k, k)$ of the EKF filtering model is given by equation 2. If initial estimates of covariance of the phase noise and covariance of noise in the measurements are wrong, then the converging time would be longer.

The EKF works in two steps, namely Prediction, and Update.

*1) Prediction*

The predicted phase of the system is obtained by,

$$m_k^- = f\,(x_{k-1}, k-1)$$
$$P_k^- = F(m_{k-1}, k-1)\,P_{k-1}F^T(m_{k-1}, k-1) + q_{k-1} \qquad (4)$$

$F(m_{k-1}, k-1)$ is the Jacobian matrix of the function $f$ and $q_{k-1}$ is the process noise covariance.

The Jacobian function $F(m_{k-1}, k-1)$ is given by,

$$F(m_{k-1}, k-1) = \left|\frac{\partial f\,(x_{k-1}, k-1)}{\partial x}\right| \qquad (5)$$

*2) Update*

From the estimated phase of the system, the estimated measurement of the system is given by the measurement function $h\,(x_k, k)$.

The error between the actual measurement of the system and the estimated measurement of the system using measurement function is given by,

$$e_k = z_k - h\,(x_k, k) \qquad (6)$$

where $z_k$ is the actual measurement value of the system.

The Kalman gain is used to denote the weightage of uncertainty between noisy measurement and predicted estimate of the system based on the measurement function given in equation 2.

The Kalman Gain in EKF is calculated by,

$$K = P_k^- H^T\,(HP_k^- H^T + r))^{-1} \qquad (6)$$

where K is the Kalman Gain, r is the measurement noise covariance. H is the Jacobian matrix of the measurement function $Y_k$. The Jacobian function H is given by,

$$H(m_k, k) = \left| \frac{\partial h(x_k, k)}{\partial x} \right| \quad (7)$$

Using the Kalman gain function, updated prediction is obtained as follows,

$$m_k = m_k^- + Ke_k$$
$$P_k = (I - KH)P^- \quad (8)$$

The new updated values are fed into the prediction stage during the next iteration. Using the above equation, Extended Kalman Filter is able to predict the system without knowing the system parameters. The convergence time of the system is dependent on the correctness of initial estimates of the parameters. The proposed EKF algorithm is implemented in python using the inputs obtained from the reference pulses arm in optical simulation. The EKF algorithm is implemented as shown in figure 1.

**PREDICTION:**

$$m_k^- = f(x_{k-1}, k-1)$$

$$P_k^- = F(m_{k-1}, k-1)P_{k-1}F^T(m_{k-1}, k-1) + Q_{k-1}$$

**UPDATE:**

$$e_k = z - h(x_k, k)$$
$$K = P_k^- H^T (HP_k^- H^T + R))^{-1}$$
$$m_k = m_k^- + Ke_k$$
$$P_k = (I - KH)P^-$$

## IV. SECRET KEY RATE ANALYSIS

In Gaussian-Modulated CV-QKD, Alice prepares the coherent states $|\alpha> = |X_A + iP_A>$, where $X_A$ and $P_A$ are quadrature values drawn from a set of normally distributed random variables with mean zero and covariance $V_A$. Alice transmits a sequence of states to Bob over an insecure transmission channel. The transmission channel is assumed to be in complete control of the eavesdropper Eve. Bob randomly chooses to measure either quadrature X or quadrature P. He then informs Alice of his measurements from which they compute the mutual information that Alice and Bob share and the amount of information that has been leaked to Eve. If the mutual information between Alice and Bob is less than the amount of information that has been leaked to Eve, i.e., the maximum information between Eve and Bob that is bound by Holevo information, the protocol is aborted. Else, Bob and Alice perform error correction and privacy amplification.

The final secure secret key rate for reverse reconciliation under collective attack is given by,

$$\delta I = \gamma I_{AB} - \chi_{BE`} \quad (9)$$

where, $I_{AB}$ is the mutual information between Alice and Bob, $\gamma$ is reconciliation efficiency and $\chi_{BE`}$ is the maximum information between Eve and Bob that is bounded by Holevo information. As explained above, the mutual information between Alice and Bob combined with reconciliation efficiency should be higher than $\chi_{BE`}$.

The mutual information between Alice and Bob can be expressed as,

$$I_{AB} = \frac{1}{2}\log_2 \frac{V + \chi_{tot}}{1 + \chi_{tot}} \quad (10)$$

where, $V = V_A + 1$ and total noise denoted by $\chi_{tot}$ can be calculated as

$$\chi_{tot} = \chi_{line} + \chi_{ohm}/T \quad (11)$$

$\chi_{ohm}$ stands for noise from homodyne detection and $\chi_{line}$ stands for noise from the channel, and T is the channel transmittance. For an attenuation co-efficient $\alpha$, the channel transmittance T is given by $10^{-\alpha L/10}$ for transmittance distance L.

The total noise from the channel is given by,

$$\chi_{line} = 1/T - 1 + \varepsilon \quad (12)$$

The excess noise of the system is denoted by $\varepsilon$. The excess noise is given by,

$$\varepsilon = \varepsilon_\phi + \varepsilon_r \quad (13)$$

In the above equation, the phase noise of the system is given by $\varepsilon_\phi$ and the noise due to Raman scattering of photons is given by $\varepsilon_r$.

Let us assume that the phase of the quantum signal to be $\phi_s$. The signal of the LO at reception is given by $\phi_{LO}$. The difference between the phase of the signal at LO and quantum signal is given by,

$$\phi_{error} = \phi_{LO} - \phi_s \quad (14)$$

$\phi_{error}$ in our case is the phase error that we have obtained from our EKF estimation algorithm. In reverse reconciliation scheme, Alice's data has to be corrected with the help of a rotation matrix that is defined by,

$$\begin{pmatrix} \cos\phi_{err} & \sin\phi_{err} \\ -\sin\phi_{err} & \cos\phi_{err} \end{pmatrix} \quad (15)$$

Alice's corrected data is given by the covariance matrix,

$$\begin{pmatrix} \widetilde{x_A} \\ \widetilde{p_A} \end{pmatrix} = \begin{pmatrix} \cos\phi_{err} & \sin\phi_{err} \\ -\sin\phi_{err} & \cos\phi_{err} \end{pmatrix} \begin{pmatrix} x_A \\ p_A \end{pmatrix} \quad (16)$$

Assuming that the phase noise arising is gaussian, the estimated phase noise can be written as [16],

$$\varepsilon_\phi = 2V_A(1 - e^{-V_{est}/2}) \quad (17)$$

In the equation above, $V_A$ stands for covariance of Alice's quadrature modulation. The term $V_{est}$ is the phase noise of the system given in equation 1.

In order to increase the secret key rate, the phase noise of the system should be kept minimal. The phase noise of the system is due to two different components. The phase error stems from phase estimation error and from the relative phase drift between two free-running lasers. The equation for calculating phase estimation error is shown in equation 14.

The noise from homodyne detection can be defined as,

$$\chi_{hom} = (1 - \eta + \nu_{ele})/\eta \quad (18)$$

$\nu_{ele}$ denotes electronic noise and $\eta$ is the efficiency of the detector.

From the above equations, Holevo information $\chi_{BE`}$ can be calculated as follows.

$$\chi_{BE`} = G\left(\frac{\lambda_1 - 1}{2}\right) + G\left(\frac{\lambda_2 - 1}{2}\right) - G\left(\frac{\lambda_3 - 1}{2}\right) - G\left(\frac{\lambda_4 - 1}{2}\right) \quad (19)$$

where the function of G is given by,

$$G(x) = (x + 1)\log_2(x + 1) - x\log_2(x) \quad (20)$$

The procedure for calculating the value of $\lambda_1, \lambda_2, \lambda_3, \lambda_4$ is shown in the appendix.

## V. Simulation for Performance Analysis

The performance of the EKF algorithm at varying linewidths is shown in Table 1.

| Initial Phase | Line Width | Iterations | Phase Error |
|---|---|---|---|
| 0.750492 | 100 KHz | 70 | 0.000178 |
| 0.750492 | 50 KHz | 50 | 0.000183 |
| 0.750492 | 10 KHz | 30 | 0.000273 |
| 0.750492 | 2 KHz | 9 | 0.000118 |
| 0.750492 | 0.1 KHz | 5 | 0.000416 |

**Table 1.** *The average phase error obtained through the use of the EKF phase estimation algorithm at different line widths along with the number of iterations taken for convergence.*

| SNR in dB | Iterations | Phase Error |
|---|---|---|
| 6 dB | 70 | 0.000178 |
| 10 dB | 140 | 0.000855 |
| 14 dB | 200 | 0.000879 |

**Table 2.** *The average phase error and number of iterations it takes for convergence for various SNR values in dB. All the calculations were performed in 50 kHz line width.*

The phase error was calculated for different line widths when the signal was passed through an optical fiber of length 20 km. It can be seen from the table above that the time that it takes for convergence of the EKF filter depends upon the linewidth of the laser pulses. The number of iterations that the filter takes for convergence increases with line width. On average, the phase error obtained through EKF phase estimation is around the factor of $10^{-4}$.

The performance of the EKF phase estimation algorithm at various Signal to Noise Ratios (SNR) values in dB is shown in Table 2. The performance of the EKF algorithm degrades at low SNR values and performs better with an increase in SNR value. The number of iterations that it takes for convergence increases with a decrease in SNR values. The phase error, on the other hand, remains around the factor of $10^{-4}$.

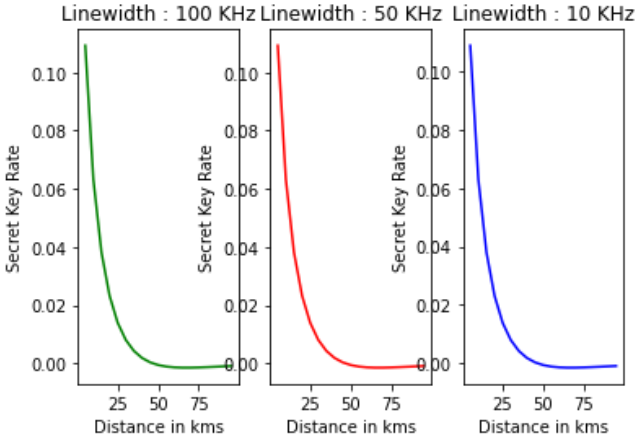


***Figure 2.*** *Results of secret key rate at various lidewidths of the laser with different phase errors obtained after EKF estimation as shown in Table 1.*

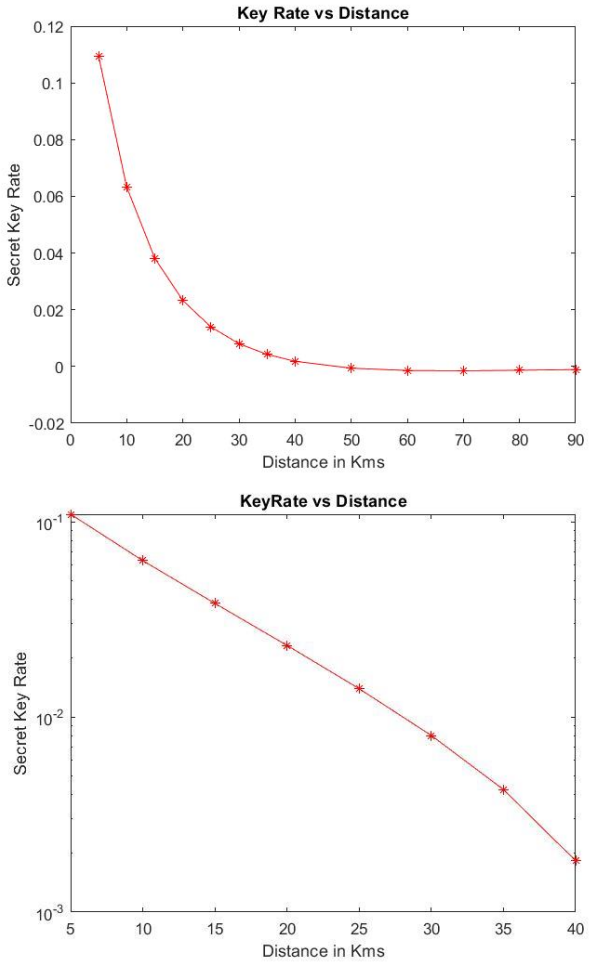


***Figure 3:*** *Results of final secret key rate at various distances for line width of 100 KHz.*

From the secret key rate analysis given above, the secret key rate of phase estimation using EKF scheme was analysed for different linewidths of the laser. The results of the simulation is plotted in Figure 2. The parameters are assumed for calculation as follows. The value of attenuation coefficient to calculate the value of T is assumed to be $\alpha$ = 0.2 dB/km. The value of variance chosen for calculation is $V_A$ = 2.5. The reconcilation efficiency $\beta$ is set to be at 90% (0.9). The detector efficiency $\eta$ is set to be 0.6. The electronic noise from the detector is assume to be $v_{ele}$ = 0.1. From figure 2, it can be seen that the EKF estimation algorithm performs similarly at various linewidths of the laser. Figure 2. shows the secret key rate at line width of 100 KHz at various tranmissting distances. The parameters assumed are the same.